PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-219044
(43)Date of publication of application : 12.09.1988

(51)Int.Cl. G06F 12/14

(21)Application number : 62-052521
(22)Date of filing : 06.03.1987

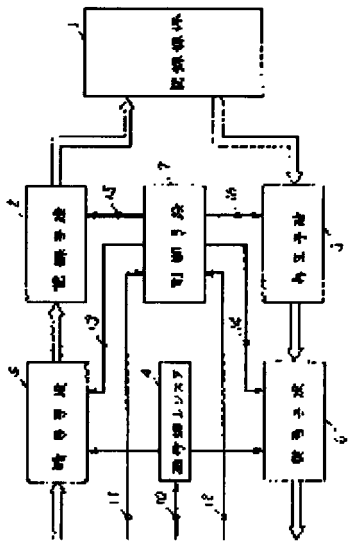
(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NAKANO YOSHIO

(54) INFORMATION STORAGE DEVICE

(57)Abstract:

PURPOSE: To protect an information, and at the same time, to easily perform the copy of a medium as in the past by writing in the information in an information recording area after encoding it into a cipher by the code of a cipher key register, and making the information difficult to understand, at the time of the recording of the information.

CONSTITUTION: When a data is written in the recording medium, the code for encoding it into the cipher is set in the cipher key register 4. An encoding means 5 encodes the written data into the cipher by using the contents of the register 4 by the control of a controlling means 7, and a recording means 2 writes in the encoded data in the medium 1. When the data is read out, the code for decoding is set in the cipher key register 4. The controlling means 7 requests the information from an objective sector, and a reproducing means 3 reads out the encoded data from the medium 1 and sends it to a decoding means 6. The decoding means 6 decodes the read out data by the contents of the register 4, and restores and transmits the data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－219044

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)9月12日
G 06 F 12/14	320	B－7737－5B	

審査請求　未請求　発明の数 1　（全4頁）

⑤4発明の名称　情報記憶装置

⑳特　願　昭62－52521
㉒出　願　昭62(1987)3月6日

⑦2発明者　中埜　善夫　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦1出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
⑦4代理人　弁理士　中尾　敏男　外1名

明　細　書

1、発明の名称

情報記憶装置

2、特許請求の範囲

(1)　記録媒体上に形成される情報記録領域に情報を書き込む記録手段と、前記情報記録領域から情報を読み出す再生手段と、暗号鍵レジスタと、情報を暗号化する暗号手段と、暗号化された情報を復号する復号手段と、情報記録時には前記暗号鍵レジスタ内の符号により前記暗号手段で情報を暗号化したのち前記記録手段により情報を前記情報記録領域に書き込み、情報再生時には前記再生手段により前記情報記録領域から情報を読み出したのち前記暗号鍵レジスタ内の符号により前記復号手段で情報を復元するよう制御する制御手段を具備することを特徴とする情報記憶装置。

(2)　暗号手段および復号手段が、暗号鍵レジスタが非暗号化を指示しているときは情報に何の操作も施さない機能を有することを特徴とする特許請求の範囲第1項記載の情報記憶装置。

3、発明の詳細な説明

産業上の利用分野

本発明は計算機装置の二次記憶などに用いられる情報記憶装置に関し、記録された情報が不正に盗用されるのを防ぐ機能を有するものである。

従来の技術

従来の情報記憶装置としては、磁気テープ、磁気ディスク、磁気ドラムを利用したものがあるが、その機能性、操作性から磁気ディスクが多く使用されている。交換可能（可搬）な媒体は、オフラインの状態ではＯＳなどによるコンピュータ管理からはずれるため、機密上その管理が重要となる。計算機センターなどでは、媒体の管理は厳重になされているので、むしろオンライン時の悪意をもったユーザからの不正なアクセスや不慮の破壊からの防御の方が問題になる。これには、ユーザIDによってファイルをアクセスする権利があるかどうかを判定するのが一般的である。

それとは別に、近年は、パーソナルコンピュータが普及し、可搬な磁気ディスクであるフロッピ

ーディスクが定着している。現存のパーソナルコンピュータ・システムでは、ユーザ管理つまり登録制度が不要であり、すべてのユーザは対等となっている。情報をフロッピーディスクに格納しておけば、同一の機器でなくても同種の他の機器でも処理が継続でき使い勝手がよい。このときフロッピーディスクは、明示的に機器使用中の情報記憶装置として使用されるだけでなく、暗示的に情報の保存や受け渡しの媒体としても使われていることになる。つまり、オンライン、オフラインの切換が容易であり、しかもその区別が曖昧である。したがって、媒体の保管管理は個人に依存しているのが現状である。

このようなパーソナルコンピュータ・システムでは、ユーザ識別によってファイルのアクセス権を管理するのは難しく、むしろファイル自体に保護をかけるのが有効である。例えば日本公開特許開昭５８－１７８４５６による「磁気ディスク制御装置」においては、磁気ディスクのセクタごとにパスワード領域とデータ領域を設け、パスワードが一致しないとデータをアクセスできない装置を考案している。また、UNIXのedコマンドは－xオプションの指定により、ファイルからのデータの入出力ごとに復号と暗号を繰り返している。

発明が解決しようとする問題点

しかしながら、第１の引用例の装置による保護では、セクタによって異なるパスワードを付与しているとバックアップディスクの作成（媒体の信頼性や誤消去からの復旧のために屢々行なう）時のパスワード入力に問題がある。つまり、パスワードに拘らずデータを複写する機能を提供すると、パスワードそのものの存在価値がなくなる。また既存のディスクデータとは互換性がない。

また、第２の引用例のようにアプリケーション・ソフトウェアで個別に行なうと、すべてのアプリケーションが対処しなければならなくなり、現在までに蓄積されたソフトウェアも対応させるのは困難である。

本発明はかかる点に鑑み、既存のソフトウェア、既存のディスクにも適用できる、情報保護機能を備えた情報記憶装置を提供することを目的とする。

問題点を解決するための手段

本発明は、情報記録領域に情報を書き込む記録手段と、情報記録領域から情報を読み出す再生手段と、暗号鍵レジスタと、情報を暗号化する暗号手段と暗号化された情報を復号する復号手段と、それらを制御する制御手段を備えた情報記憶装置である。

作　用

本発明は前記した構成により、情報記録時には暗号鍵レジスタの符号により情報を暗号化したのち情報記録領域に書き込むことにより難解化するものである。

実　施　例

第１図は本発明の一実施例における情報記憶装置のブロック図を示すものである。第１図において、１は記録媒体、２は記録手段、３は再生手段、４は暗号鍵レジスタ、５は暗号手段、６は復号手段、７は制御手段である。

以上のように構成された本実施例の情報記憶装置について、以下その動作をフローチャートにしたがって説明する。本実施例では説明上、記録媒体上に形成される情報記録領域をセクタとする。

第２図はデータの書き込み動作を示したフローチャートである。

（W1）　暗号化のための符号Kwtが、暗号鍵設定信号線１０により暗号鍵レジスタ４に設定される。

（W2）　データ書き込み制御信号線１１により目的とするセクタへの情報の書き込みを要求する。

（W3）　制御手段７は暗号要求を暗号信号線１３に出す。

（W4）　暗号手段５は書き込みデータ暗号鍵レジスタ４の内容Kwtで暗号化し、記録手段２に送出する。

（W5）　制御手段７は書き込み要求を記録信号線１５に出す。

（W6）　記録手段２は暗号化されたデータを記録媒体１に書き込む。

第３図はデータの読み出し動作を示したフローチャートである。

（R1）　復号のための符号Krdが、暗号鍵設定信号線１０により暗号鍵レジスタ４に設定される。

（R2）　データ読み出し制御信号線１２により目的とするセクタからの情報の読み出しを要求する。

（R3）　制御手段７は読み出し要求を再生信号線１６に出す。

（R4）　再生手段３は暗号化されたデータを記録媒体１から読み出し、復号手段６に送出する。

（R5）　制御手段７は復号要求を復号信号線１４に出す。

（R6）　復号手段６は読み出されたデータを暗号鍵レジスタ４の内容Krdで復号し、データを復元する。

暗号手段５および復号手段６は、暗号鍵レジスタ４の内容が非暗号化を指示しているときは何の操作も加えない機能を有しているので、暗号化の有無に拘らずバックアップディスクを作成することができ、また、既存の非暗号化データも従来通り扱うことができる。さらに、制御手段７に１回のデータの書き込み動作／読み出し動作終了ごとに暗号鍵レジスタ４の内容を非暗号化指示状態にする機能をもたせれば、マルチプロセス環境下での暗号鍵符号の混合を避けることができる。

発明の効果

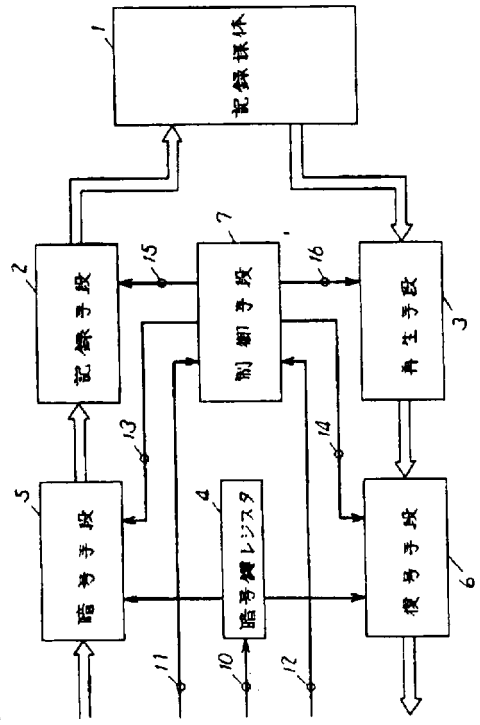
以上説明したように、本発明によれば、媒体の復写も従来通り容易に行なえるが、情報の保護も果たされる。また装置内で暗号化を行なうので、既存のソフトウェアを大幅に修正することなく保護機能を利用でき、その実用的効果は大きい。

４、図面の簡単な説明

第１図は本発明における一実施例の情報記憶装置のブロック図、第２図は同実施例における書き込み動作を示すフローチャート、第３図は同実施例における読み出し動作を示すフローチャートである。

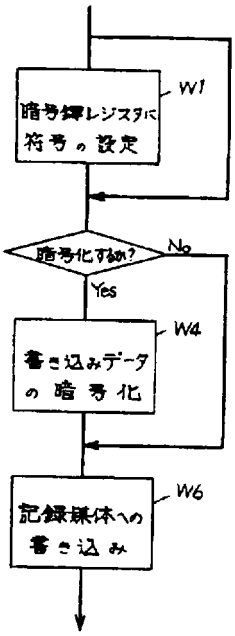
１……記録媒体、２……記録手段、３……再生手段、４……暗号鍵レジスタ、５……暗号手段、６……復号手段、７……制御手段。

代理人の氏名　弁理士　中　尾　敏　男　ほか１名

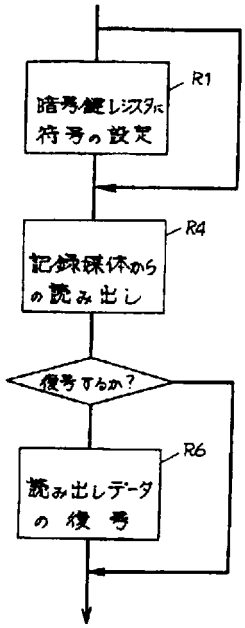


第１図

第 2 図


W1
暗号鍵レジスタに
符号の設定
暗号化するか?
No
Yes
W4
書き込みデータ
の暗号化
W6
記録媒体への
書き込み

第 3 図


R1
暗号鍵レジスタに
符号の設定
R4
記録媒体から
の読み出し
復号するか?
R6
読み出しデータ
の復号